Effective February 2, 2026. These Service Descriptions supersede and replace all prior versions.

Schedule of Services

The Services to be performed for Client by Provider are set forth in the Order. Additional Services may be added only by entering into a new Order including those Services.

Provider, through its Third-Party Services Providers will make its best effort to ensure the security of Client's information through third-party security software ("Security Software"). Client designates Provider as its agent to provide the Service to Client, and to enter into any third-party relationship to provide the Service to Client. Use of this Service is subject to the applicable Third-party Service Providers agreements regarding terms of use, which Client and Provider agree has been provided by Provider to Client. Client acknowledges that Third-Party Service Providers and their licensors own all intellectual property rights in and to the Security Software. Client will not engage in or authorize any activity that is inconsistent with such ownership. Client acknowledges and agrees to be bound by any applicable Third-Party Service Provider agreements regarding terms or use or end user licensing terms, and Client understands that any applicable agreement regarding terms of use or end user licensing is subject to change without notice.

Essential IT & Basic Security (EIT)

Essential IT initiates the RIC Master Plan launch by using Agents and Network Collectors that will **R**emotely **M**onitor your entire infrastructure and provides NDS the ability to perform routine infrastructure **M**aintenance to monitor, uncover, and identify deficiencies in our **Clients'** environment.

DELIVERABLE	OUTCOME
Patch Management**	Keeps systems running optimally and properly patched with security updates. Automatically patches Servers and Workstations based on published **C**ommon **V**ulnerabilities and **E**xposures (CVEs).
Antivirus, Ransomware protection	Detects, identifies, and isolates common threats to endpoints devices—including viruses, malware, and ransomware using advanced behavior analysis. Sophisticated Cyberthreat Analysis Managed Operations Center 24/7 and advanced AI analysis.
Managed Detection and Response (MDR 24x7 SOC)	Managed SOC 24/7 Threat Monitoring. Around the clock protection with real-time advanced threat detection. We catch sophisticated and advanced threats that bypass traditional AV and perimeter security solutions. An elite cybersecurity team proactively hunts for malicious activities so you can focus on other pressing matters.

Network Topology Mapping	Network and IoT devices are everywhere and need to be managed— and managing the network starts with understanding what's out there.
Communications and Workflow	Proven and ready to implement guidelines, procedures, and audit trails for response times, ticket management, incident reporting, trouble-ticket escalation, and all that stuff that takes years to build.
Executive Level Reporting	Know the overall health and lifecycle of your assets within your organization.
Device Discovery & Asset Management	Real-time visibility of every asset —where it is, status, condition, and compliance.

Essential IT & Basic Security BENEFITS

- Launch RIC Master Plan with healthy, stabilized computing environment.
- Prevent confusion, chaos, and stress during initial RIC deployment &
- Direct identification of highest-risk vulnerabilities.

Co-Managed IT - Secure Foundation (MIT)

Co-Managed IT (MIT) Includes Essential IT & Basic Security (EIT). MIT fulfills our **Clients's** fundamental requirements for secure, reliable digital operations by providing a core set of ongoing IT management services.

DELIVERABLE	RESULT
Remote Remediation	Instantly responds to alerts, incidents and fixes critical issues that could compromise access to critical systems and/or disrupt user productivity relating to compute processes.
Basic M365 and Google Workspace Management	Stop worrying about needing to become an expert on your email platform. Let us do the heavy work for you.
IT Policy & Procedure(s)**	Customizable templates designed to fulfill requirements in a way that's easy for everyone to understand
IT Documentation/Collaboration**	Easy collaboration of all IT Systems, documentation, Vendor platforms, and passwords in one easy location customizable sharing between our team and yours.
Server Password management**	Prevents your users from hindering your organization's security and opening the door for hackers. Facilitates best practices: password encryption, strong passwords, password generation, frequent password changes, off-device password storage, etc.

Password Sync with AD and O365	One password change. Easy to reset both at the same time.
Basic Cloud Backup for Servers**	Daily cloud backups for your critical servers.
Lifecycle Asset Management	Easy CapEx Budget reporting on the lifecycle and replacement cost(s) of your IT assets

Co-Managed IT – Secure Foundation BENEFITS

- Provides optimal productivity all day, every day.
- Reduces exposure to technology-related risks.
- Protects against extended business interruption and/or data loss.
- Reaps higher technology return-on-investment (ROI).
- Offloads non-strategic IT-related work.

*Note: Managed IT / Basic Security does not include support for our **Clients**'s business applications. our **Clients** will continue to utilize the technical support provided by those software vendors directly. However, in situations where a business application issue may involve Clients's IT infrastructure, **NDS** will collaborate with those vendors to help resolve the issue.*

CyberWatch

Comprehensive Risk and Vulnerability Identification

(Independent 3rd Party Cybersecurity Assessment-as-a-Service)

NDS strongly recommends that our **Clients** utilize our **Independent Third-Party** cybersecurity assessment service in conjunction with this Risk Intelligence and Countermeasures (RIC) Master Plan.

DELIVERABLE	RESULT
Penetration test(s) 4x Annually**	Tests cyber defenses by performing emulated hacker attacks via external vectors and/or as a malicious insider
Vulnerability analysis	Thorough inspection of digital environment to detect shortcomings in settings, configurations, and policies
CVE analysis	Detects failures to apply software patches and updates that are necessary to prevent known exploits
PII Analysis	Advanced scans for unencrypted personally identifiable information (PII) that poses security and/or compliance risk
User Hygiene Analysis	Looks for indicators of problematic user behaviors such as weak passwords, website cookies, stored tokens, etc.
Digital Health Report	Provides detailed, itemized documentation of discovered issues along with checklist of suggested remediations

THIRD-PARTY ASSESSMENT BENEFITS

- High-value diagnosis of current security posture.
- High-value guidance for a Great Start execution provided by initial assessment.

- Periodic assessments measure RIC Master Plan performance/progress over time.
- A complete and **Objective Third-Party Audit** that is required for Regulators, Cyber Insurance Underwriters, Customers, and Others.

Cyberwatch Advanced - Proactive Advanced Security (PAS)

Proactive Advanced Security provides our **Clients** with the ongoing enterprise-caliber cyber defense that every organization needs to protect itself against the ever-escalating volume of attacks being perpetrated by relentlessly inventive hackers, malicious state actors, and cybercriminals who can now inexpensively resource ransomware, reputational blackmail, and other exploits via open markets on the dark web.

DELIVERABLE	RESULT
Independent 3rd Party Assessment *CyberWatch***	Ongoing every Qtr (4x per year) you receive an Independent 3rd Party Assessment.
Domain & Email Protection**	Domain and Email protection by automating the implementation of DMARC, SPF, and DKIM protocols, stopping unauthorized users from sending emails on your behalf. It provides full visibility into email sources, prevents phishing and spoofing attacks, increases email deliverability, and monitors for lookalike domain abuse.
Identity Access Management (IAM)	A comprehensive, cloud-based Identity and Access Management (IAM) solution that secures, manages, and automates user access to applications & devices. It provides Single Sign-On (SSO), Adaptive Multifactor Authentication (AMFA), and lifecycle management (provisioning/deprovisioning) to enforce security policies and support Zero Trust strategies for employees and vendors.

IT Documentation & Collaboration**	IT documentation platform that serves as a centralized “source of truth” to manage, secure, and standardize IT documentation and Knowledge Management.
Basic Zero Trust / Least Privilege Framework **	Allows you to control and audit privileged access and permissions for users, accounts, applications, processes, and systems using **P**rivileged **A**ccess **M**anagement.
Asset Intelligence & Audit ** Attack Surface	Attack Surface platform that provides deep visibility into IT systems across cloud, network, and SaaS applications. Automates documentation, tracks configuration changes to prevent drift, and aids in security compliance to protect against cyber threats.
User Security Training and Employee attestation**	Cybersecurity Training program for Users. Includes: Unlimited Dark Web Scanning (PII - Personal Identifiable Information), Unlimited Phishing Campaigns (Test the education of your End Users).

ADVANCED SECURITY BENEFITS

- Reduces financial, operational, and reputational risk significantly.
- Minimizes window of opportunity for attackers who penetrate perimeter defenses.
- Enhances defense against insider threats.
- Protect customers, supply chains, partners, and others more effectively.
- Fulfills requirements for superior cyber insurance coverage.
- Makes security best practices easier for employees.

Compliance-as-a-Service (CaaS)

Compliance-as-a-Service (CaaS) enables our **Clients** to achieve and maintain compliance with the growing range of increasingly complex and wide-ranging operational requirements mandated by Cyber Insurance Underwriters, Government Agencies, Industry Certification Authorities, and others.

DELIVERABLE	RESULT
Microsoft 365 hardening**	Adds anti-phishing intelligence, removal of insecure legacy protocols, detection of forged sender IDs, etc.
Workflow/approval tracking	Records approval process to document what, when, who, and why policies have been implemented.
Customized controls framework	Provides foundation for implementing 218 key controls required to support Top 20 regulatory and cyber insurance mandates.
Advanced Security training content	Provides required compliance-related cyber/physical security education for all employees and IT administrators.
Update management	Prompts for required changes when new mandates are issued and provides version control/validation.

COMPLIANCE-AS-A-SERVICE (CaaS) BENEFITS

- Dramatically reduce the burden of complying with expanding mandates.
- Avoid fines, Code of Conduct, and other penalties by keeping compliance current.
- Proof of due diligence and mitigates penalties even in the event of a violation.
- Qualify for superior cyber insurance coverage.
- Improve on-boarding of new employees.

vCSO

vCSO enables our **Clients** to reap the benefits of having a Chief Security Officer while avoiding the costs and risks associated with executive search, recruitment, compensation, retention, and turnover. These are especially significant given the extreme global shortage of experienced, qualified cybersecurity professionals at this level.

DELIVERABLE	RESULT
Executive oversight	Unified command-and-control of critical security, compliance, and related RIC functions
Transformational leadership	Elevates efforts from operational/tactical to instill a true organizational culture of security and compliance
Risk-driven prioritization	Helps ensure that resources are allocated to the most important/pressing compliance first
C-level strategy and Road Mapping	Enables upper management and board to make strategic fact-based decisions about risk appetite, risk/reward, etc.
Management perspective/collaboration	Go-to resource for managers who need to factor expert insights about threat and risks into their decision-making

vCSO BENEFITS

- Essential business advantages of a CSO without the costs of a CSO
- Proactive, strategic approach to mitigating organizational risk
- Security and compliance integrated into executive-level decision-making
- Maximum value from internal and external resources
- Improved insurability profile
- High-impact item checked off on audit/regulatory scorecard

Add-Ons

Add-Ons enables our **Clients** to expand upon the above service offerings.

DELIVERABLE	RESULT
Business Continuity Disaster Recovery (BCDR)**	Hourly Server backups with rapid local restoration capabilities with off-premises cloud replication that are tested & validated.
M365 Cloud Backup**	Protects your user mailbox(s), cloud drives, from costly mistakes and/or malicious behavior.
24x7 Help Desk	Skilled technical support available for remote assistance 24×7. Help Desk is your dedicated support center, ready to assist your team around the clock via email, phone, and chat.
NOC 24x7 Server Support & Maintenance	Peace of mind knowing that our **N**etwork **O**perations **C**enter is dedicated to the proper and daily operation and maintenance of your servers and network 24x7x365.
Adaptive Multi-Factor Authentication**	Reduce the risk of account takeovers and provide additional security to users and your environment.
Advanced Whitelisting / Zero-trust Framework**	Keeps users from running scripts. Stop worrying about employees rolling out the red carpet for hackers.
Endpoint Cloud Backup	Protects your Workstations, Operating Systems, and Applications from costly mistakes and/or malicious behavior.
Voice Over IP (VoIP)	Next Generation VoIP with Unified Communications, Mobile Integration, Video Conferencing, etc.
CyberVault Encrypted Enclave**	Least Privilege & Zero Trust Encrypted Enclave for Storage & Collaboration. Encrypted Platform (FEDRAMP Certified) to Store & Share Data. Meets requirements for CMMC/NIST 800-171, DFARS, PCI, SEC, FTC.
CyberLog Encrypted SIEM**	All-in-one, cybersecurity platform that combines Security Information and Event Management (SIEM), advanced vulnerability scanning, and automated inventory tracking to meet CMMC, NIST, DFARS, SEC, FTC compliance.

** Accepted by most Cyber Insurance Underwriters. Required by SEC / FTC / PCI / HIPPA / CMMC

*Provider does not provide internet connection. Client is responsible for providing internet connection to use the Service.

THESE DESCRIPTIONS ARE SUBJECT TO CHANGE ANY TIME WITHOUT NOTICE.